UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/578,633	05/25/2000	Steven Branigan	1-1-7	5753

7590 12/10/2003

Docket Administrator Rm 3C 512
Lucent Technologies Inc
600 Mountain Avenue
P O Box 636
Murray Hill, NJ 07974-0636

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	PAPER NUMBER
2131	2

DATE MAILED: 12/10/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/578,633	BRANIGAN ET AL.	
	Examiner	Art Unit	
	Michael R Vaughan	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 May 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 May 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claims 1-27 have been examined and are pending.

Claim Rejections - 35 USC ' 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless --

> the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

Claims 1-3, 5-12, and 15-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Shostack et al (USP 6,298,445).

As per claims 1 and 24, Shostack et al teach a communications network security method comprising:

identifying a plurality of routes that define the communications network (column 12, lines 41-57);

identifying a plurality of hosts as a function of the plurality of routes (column 12, lines 41-57);

performing a census of the communications network as a function of the plurality of hosts to determine a topology of the communications network (column 12, lines 41-57);

probing at least one host of the plurality hosts by transmitting a packet to the host, the host being selected from the census results and the packet having at least a source address determined as a function of the topology (column 12, lines 41-57); and

determining a security characteristic of the probed host as a function of a response by the probed host in receiving the packet (column 12, lines 41-57).

As per claims 2 and 25, Shostack et al teach the source address is an IP address associated with a host external to the communications network and the packet is

constructed as a function of the source address and an IP address associated with the at least one host (column 1, lines 64-65 and column 3, lines 1-4).

As per claims 3 and 26, Shostack et al teach the response of the probed host to the receipt of the packet includes transmitting a second packet, the second packet being derived using at least a portion of information from the received packet (column 5, lines 20-35).

As per claim 5, Shostack et al teach the probing the at least one host operation further comprises:

identifying the IP address associated with the probed host from the census (column 12, liens 41-55); and

generating the packet as a function of the IP address associated with the probed host and the IP address associated with a host external to the communications network (column 1, lines 64-65).

As per claim 6, Shostack et al teach the determining the security characteristic operation further comprises:

monitoring the probed host to determine the response, and if the response includes a transmission of a second packet from the probed host, generating a security alert message identifying the probed host as a security risk (column 7, lines 5-19).

As per claim 7, Shostack et al teach the second packet is derived using at least a portion of information from the transmitted packet (column 5, lines 24-45).

As per claim 8, Shostack et al teach the transmitted packet is a TCP packet (column 5, lines 24-45).

As per claim 9, Shostack et al teach the second packet is a UDP packet or an ICMP packet (column 5, lines 24-45).

As per claim 10, Shostack et al teach a method for analyzing network security of a communications network, the method comprising:

identifying a plurality of routes that define the communications network (column 12, lines 41-57);

identifying a plurality of hosts internal to the communications network as a function of the plurality of routes (column 12, lines 41-57);

performing a census of the communications network as a function of the plurality of hosts to determine a topology of the communications network (column 12, lines 41-57);

transmitting a packet from a host external to the communications network to a particular one host of the plurality of hosts internal to the communications network, the internal host being selected from the census, and the packet being

generated as a function of an IP address associated with the host external to the communications network and an IP address associated with the particular one host of the plurality of hosts internal to the communications network (column 13, lines 1-6); and

determining a security characteristic of the particular one internal host as a function of a response by the internal host to the receipt of the packet (column 12, lines 41-57).

As per claim 11, Shostack et al teach the determining the security characteristic operation further comprises:

monitoring the probed host to determine the response, and if the response includes a transmission of a second packet from the probed host, generating a security alert message identifying the probed host as a security risk (column 7, lines 5-19).

As per claim 12, Shostack et al teach the second packet is derived using at least a portion of information from the transmitted packet (column 5, lines 24-45).

As per claim 15, Shostack et al teach the security characteristic includes an indication that the probed host is outside any security measures provide by a firewall associated with the communications network (column 9, lines 10-18).

As per clam 16, Shostack et al teach A communications system comprising:

a first plurality of computers associated with a first communications network;

a second plurality of computers associated with a second communications network; and

a security host computer which determines a security characteristic of a first computer from the plurality of computers, performs a census of the communications network as a function of the first plurality of computers, and probes the first computer by transmitting a packet to the first computer, the first computer being selected from the census results and the packet being generated as a function of an IP address associated with a second computer of the second plurality of computers and an IP address associated with the first computer, and determining a security level associated with the first computer as a function of a response of the first computer to receiving the packet (column 12, lines 41-57, column 1, lines 64-65, and column 3, lines 1-4).

As per claim 17, Shostack et al teach the security host computer is associated with the first communications network (column 4, lines 33-34).

As per claim 18, Shostack et al teach the response of the probed host to the receipt of the packet includes transmitting a second packet, the second packet being

derived using at least a portion of information from the received packet (column 5, lines 20-35).

As per claim 19, Shostack et al teach the determining the security characteristic operation further comprises:

monitoring the probed host to determine the response, and if the response includes a transmission of a second packet from the probed host, generating a security alert message identifying the probed host as a security risk (column 7, lines 5-19).

As per claims 20 and 27, Shostack et al teach the first communications network is an intranet and the second communications network is an Internet (column 4, lines 14-21).

As per claim 21, Shostack et al teach a security host computer comprising:

means for performing a census of a communications network and determining a topology of a first communications network, the topology being defined by at least one computer (column 12, lines 41-57);

means for probing the at least one computer by transmitting a packet to the computer, the computer being selected from the census results and the packet being generated as a function of the topology, an IP address associated with a particular host computer associated with a

second communications network and an IP address associated with the computer, the second communications network being separate from the first communications network (column 12, lines 41-57); and

a monitor for determining a security level of the computer as a function of a response by the computer to the receipt of the packet (column 12, lines 41-57).

As per claim 22, Shostack et al teach the determining the security characteristic operation further comprises:

monitoring the probed host to determine the response, and if the response includes a transmission of a second packet from the probed host, generating a security alert message identifying the probed host as a security risk (column 7, lines 5-19).

As per claim 23, Shostack et al teach the security level is determined with respect to a firewall located between the first communications network and the second communications network (column 4, lines 14-21).

Claim Rejections - 35 USC ' 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al.

As per claims 4 and 13, Shostack et al teach the performing the census operation further comprises:

> pinging a plurality of IP addresses to verify their respective validity , the plurality of IP addresses being identified from the plurality of routes (column 12,

lines 41-57);

pinging particular hosts of the plurality of hosts to verify their respective location in the topology of the communications network (column 12, lines 41-57). Shostack is silent in explicitly disclosing:

performing at least a first DNS lookup for at least one of the particular hosts; and

performing at least a second DNS lookup across a communications channel, the communications channel serving to connect the communications network with a network external to the communications network, the second DNS lookup identifying a specific host of the plurality of hosts.

Shostack et al teach that all IP ports are probed to see if they are weaknesses (column 12, lines 50-55). One skilled in the art knows that port 53 is DNS. Therefore, if all ports are tested for security flaws, port 53 is tested. Shostack et al also teach that remote sources can also test the security of the network by trying to probe internal hosts (column 13, lines 1-5). One skilled in the art would not want internal hosts responding to DNS packets.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Shostack et al by performing both internal and external DNS probes because internal hosts should not respond to DNS lookups because they should not reveal information about the network in which they reside. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al in view of Sitaraman et al (USP 6,212,561).

As per claim 14, Shostack et al teach that all known security attacks are stored in a database so they can be tested against the host of an intranet (column 2, lines 48-60). Shostack et al's teachings disclose a method that protects an intranet from the Internet. Sitaraman et al teach that one security risk to an intranet is a multi-homed host inside of an intranet (column 3, lines 40-49). Therefore, it would be advantageous for a system that secures intranets to check the intranet for hosts that are multi-homed.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Sitaraman et al with the system of Shostack et al because it would allow the system to guard against users which try to connect to the Internet while still being connected to the secure intranet. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

Remarks

No claim is allowed.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patents:

6,182,226	Reid et al.
6,546,493	Mgdych et al.
6,108,782	Fletcher et al.
6,253,337	Maloney et al.
6,654,882	Froutan et al
6,324,585	Zhang et al.
6,205,551	Grosse

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

MV
Michael R Vaughan
Examiner
Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100